# UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

INFORMATION ASSOCIATED WITH THE KIK ACCOUNT "cabsnztrouble_6c5" THAT IS STORED AT PREMISES CONTROLLED BY MEDIALAB, INC., A COMPANY HEADQUARTERED AT 1222 6TH ST., SANTA MONICA, CA 90401

Case No. 24-M-612

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 2251(a), | Produce child pornography |
| 2252A(a)(5)(B) | Possess child pornography |

The application is based on these facts:

See Attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Julius Klevinskas

*Applicant's signature*

Julius Klevinskas, SA Homeland Security Investigations

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ *(specify reliable electronic means).*

Date: 2-1-2024

*Judge's signature*

City and state: Green Bay, Wisconsin

Magistrate Judge James R. Sickel

*Printed name and title*

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE KIK ACCOUNT "**cabsnztrouble_6c5**" THAT IS STORED AT PREMISES CONTROLLED BY MEDIALAB, INC., A COMPANY HEADQUARTERED AT 1222 6TH ST., SANTA MONICA, CA 90401. | Case No. 24-M-612 |

**AFFIDAVIT IN SUPPORT OF AN APPLICATION**
**FOR A SEARCH WARRANT**

I, Julius Klevinskas, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., an electronic communications service provider headquartered at 1222 6th St., Santa Monica, CA 90401. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a sworn law enforcement officer currently employed as a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI) and have been so employed since approximately January 2023. I am currently assigned to the Chicago Field Division – Milwaukee Resident Office (RAC). Since becoming a Special Agent, I have received specialized training in various aspects of law enforcement and my responsibilities include

conducting investigations of alleged criminal violations of federal statutes and laws. Prior to my tenure as a HSI Special Agent, I was a Diversion Investigator with the Department of Justice - Drug Enforcement Administration (DEA), Milwaukee District Office, from approximately July 2019 to January 2023.

3. Based on my training and experience, I know that individuals who engage in criminal activity using online accounts often save, store, or possess digital information, data, and evidence within their online accounts. I know that as a regular course of business, many electronic communication service providers maintain said digital information and content for a period of time, and make it available to law enforcement agencies to seek with service of a legal Court Order. I also know that as a regular course of business, electronic communication service providers may maintain internal records that the company may collect from each individual user as set by the agreed upon terms of service at the time of account activation. These internal records may include various subscriber information such as IP address logs, user event time/date stamps, device identification, phone numbers, email addresses, etc.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251(a), which makes it a crime to produce child pornography and 18 U.S.C. § 2252A(a)(5)(B) which makes it a crime to possess child pornography, the "subject offenses." There is also probable cause to search the information

described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

## JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b) (1) (A), & (c) (1) (A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3) (A) (i).

## DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is,

or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

e. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

f. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

g. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic,"

meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

j. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

k. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

l. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

m. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

## KIK MESSENGER APPLICATION INFORMATION

8. The following information comes from materials published by Kik, online research that I have conducted, from other law enforcement officers, as well as my training and experience. Kik Messenger, commonly called Kik, is an instant messaging mobile application ("app") from the Canadian company Kik Interactive, and available free of charge on iOS and Android operating systems. It is a social networking app that permits a user to trade and disseminate various forms of digital media while using a mobile device. Kik advertised itself as "the first smartphone messenger with a built-in browser." Kik was founded in 2009 and according to its company website was designed to "break down barriers [between operating systems] that would allow users to chat with whoever, whenever." In October 2019, Kik Interactive was purchased by Santa Monica, California based MediaLab Inc.

9. Kik Messenger is a feature within Kik that allows its users to communicate with selected persons as well as browse and share any website content with those whom the user selects while still within the Kik platform. Unlike some other messaging apps, Kik usernames—not phone numbers—are the basis for Kik user accounts. Kik usernames are unique; can never be replicated; can never be changed, may include lower and uppercase letters, numbers, periods, and underscores; and will never contain spaces, emoticons or special characters. MediaLab Inc. can use a Kik username to identify a Kik account to law enforcement.

10. Kik also allows users to exchange images, videos, sketches, stickers and even web page content by posting such content privately with individual users or publicly (on the Kik platform) with multiple individuals who belong to "Groups." Groups can hold up to 50 Kik users and are oftentimes created to discuss topics such as modern popular culture-themed ideas, as well as illicit/illegal-themed ideas.

11. Kik advises that upon service of a search warrant, the company can provide the information requested in Attachment B, including: first and last name and email address provided by the user; link to the most current profile picture or background photo; device-related information; account creation date and Kik version; birthdate and email address used to register the account; user location information; the transactional chat log; the chat platform log; photographs and videos sent or received by the user for the last 30 days; the roster log; abuse reports; email events; and registration IP address associated to the username when the account was registered, including timestamp. Kik can also provide information associated with Kik groups, including: group information log; group create log; group join and leave logs; group transactional chat log; group chat platform log; photographs and videos received by the group; and group abuse reports.

12. Based on my training and experience, I know Kik is often used for illegal purposes, including the receipt, distribution, and transportation of child pornography, because of the high degree of anonymity that is afforded to the user during the use of the Kik application.

## IDENTIFICATION AND INVESTIGATION OF THE SUBJECT ACCOUNT

14. On January 3, 2024, the Wisconsin Department of Justice Division of Criminal Investigation (WI DOJ-DCI) received a referral from the United States Homeland Security Investigations (HSI).

15. Between November 27, 2023, to January 3, 2024, HSI Special Agent (SA) Eddie Ramirez, assigned to the HSI San Antonio Field Office, conducted a forensic review of a download from a desktop computer tower seized by the San Antonio Police Department (SAPD) during a child pornography investigation on June 26, 2023. On June 26, 2023, Laura Hurd, DOB: 05/26/1992, reported her boyfriend/ex-boyfriend, Bobby E. Matjeka DOB: 12/10/1980, had child pornography on his computer. SAPD dispatched an officer(s) who observed the image(s) of child pornography on the computer and subsequently seized the desktop computer tower (hereafter referred to as the computer).

16. The SAPD obtained a search warrant for the computer on June 30, 2023. Due to a backlog of electronics requiring review, HSI took custody of the computer on or around November 17, 2023. An HSI Computer Forensic Analyst (CFA) downloaded the computer between November 17, 2023, and November 27, 2023.

17. Between November 27, 2023, to January 3, 2024, HSI SA Ramirez then analyzed and reviewed the download and found 20-30 naked images of the same prepubescent female child, which SA Ramirez determined to be consistent with child pornography/child sexual abuse material (CSAM) that originated from conversations from a Kik Username(s) Char B/cabsnztrouble and text messages from phone number 920-205-5329. The images of the prepubescent female child were sent from Char B/cabsnztrouble and 920-205-5329. The chats occurred between approximately December 2021 to June 2022.

18. SA Ramirez sent a federal summons (akin to a subpoena) to the cellular service provider for the phone number, T-Mobile, and identified the owner phone number as Charlotta Belgum, residence of 907 North Fair Street, Appleton, WI, 54911.

19. Through further investigation, Charlotta was further identified as Charlotta A.

Belgum, DOB: 04/04/1986. A social media account, believed to belong to Belgum, depicted her with a young child, who was identified by Appleton School District Records to be her 8-year-old daughter, T.H., DOB: 08/03/2015. SA Ramirez subsequently identified T.H. in the social media photographs as the same child depicted in the CSAM.

20. The WI DOJ-DCI obtained the copies of the chats reviewed by SA Ramirez. WI DOJ-DCI SA Eric Voland reviewed the images recovered by SA Ramirez and believed the images to be child pornography based on Wisconsin Statutes. Some of the images and comments from the Kik conversation are summarized below:

On December 14, 2021, Char B sent seven images of T.H. in a bathtub filled with red water. T.H. is described as being naked, has shoulder length brown hair, no pubic hair, and no breast development. In one of the images T.H. is in a crouched position looking at the camera and her vagina is exposed above the water. The next image appears to be a close-up of T.H.'s vagina area and her face is not visible.

After those seven images are sent by Char B, the following conversation occurs:

| | | |
|---|---|---|
| 12/14/21 01:41 | (Matjeka) | Mmmmmmm. Man I love her |
| 12/14/21 01:42 | Char B | I know. She's delectable…I can't get enough of her. |
| 12/14/21 01:42 | (Matjeka) | I can't either |
| 12/14/21 01:44 | Char B | She's just gorgeous and I love that she's into chokers now too |
| 12/14/21 01:45 | (Matjeka) | Yes. She will be my slave so it's only right |
| 12/14/21 01:45 | Char B | Agreed |
| 12/14/21 01:46 | (Matjeka) | I'm so horny for her |
| 12/14/21 01:47 | Char B | Me too |

21. SA Voland observed 25 images of T.H. naked in or around the bathtub in the Kik conversations between December 10, 2021, and December 27, 2021, with sexual comments in response to those images.

22. On January 3, 2024, SA Voland and SA Kadie Walusay (WIDOJ-DCI) interviewed Charlotta Belgum at the Appleton Police Department. Belgum waived her Miranda Rights and agreed to speak with the Special Agents. Belgum acknowledged that she has had phone number 920-205-5329 for about the past nine years, and she acknowledged having a Kik username of Char B. Belgum indicated she met people on the website FetLife, which is a social network for people with fetishes. Belgum indicated she would meet people on this site and then later communicate with them through text messages or Kik. SA Voland showed Belgum sanitized images and some of the conversations that SA Ramirez recovered and Belgum admitted to taking those pictures of T.H. in sexually explicit positions. Belgum admitted to sending those images to "Bobby" in Texas through text messages during conversations that were sexual in nature. Belgum also admitted to receiving CSAM images from "Bobby" because he wanted Belgum to "get turned on" by those images. Belgum admitted that she took pictures of her daughter, T.H., while in the bathtub at her home at 907 N. Fair St, Appleton, WI, and at the Great Wolf Lodge in Wisconsin Dells, with her phone and nobody else besides her took those pictures. Belgum indicated that her primary email address is cabsnztrouble@gmail.com and that email account is associated with her android phone.

23. On January 8, 2024, WIDOJ-DCI SA Jacob Chihak contacted Kik to preserve Belgum's Kik account cabsnztrouble. Kik responded that this account was banned on November 22, 2023 for posting child pornography. Kik personnel indicated they would be submitting a Cybertipline report to the National Center for Missing and Exploited Children (NCMEC).

24. On January 11, 2024, WIDOJ-DCI received CyberTipline (CT) report 184248353 from NCMEC that originated from Media Lab/Kik. The tip reported that the following account was suspected of producing child pornography:

**ESP Product/Service: cabsnztrouble@gmail.com**
**Screen/User Name: cabsnztrouble_6c5**
**Display Name: cabsnztrouble**
**ESP User ID: cabsnztrouble_6c5**

On this same date, SA Voland reviewed the CT and noted that 14 images were uploaded from this account during November 20-21, 2023, using two different IP addresses. SA Voland had previously identified confirmed images of TH and of Charlotta Belgum having claw mark tattoos on her breasts. SA Voland reviewed the images attached to this report and observed images of CSAM and described two of those images. SA Voland described image filename 01a0fefea2f953de5cc8b39f5445474b.jpg as being a close up view of breasts with claw mark tattoos on them. There is a head of what appears to be a child (with brown hair wearing a black shirt) facing and being within close proximity of her breasts. Another image filename 2ce7a5092a05398c6f9ceff63a198781.jpg shows an even closer image of what appears to be the same child's mouth touching the nipple of her breast. SA Voland concluded that the child seen in these images may possibly be one of Belgum's two 8 year old children.

## INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

25. This warrant is being sought under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to require MediaLab, Inc. to disclose to the government copies of the records and other information (including the content of

communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## CONCLUSION

26. Based on the forgoing, I request that the Court issue the proposed search warrant.

27. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

28. The government will execute this warrant by serving the warrant on MediaLab, Inc. Because the warrant will be served on MediaLab, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Dated this 1 day of ~~January~~ February 2024.

Julius Klevinskas

Julius Klevinskas
Special Agent, Homeland Security Investigations

Sworn to telephonically this 1 day of ~~January~~ February 2024.

James R. Sickel
United States Magistrate Judge

24-m-612

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with Kik username "**cabsnztrouble_6c5**" that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a company headquartered at 1237 7th St., Santa Monica, CA 90401.

## ATTACHMENT B

### Particular Things to be Seized

**I. Information to be disclosed by MediaLab, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab, Inc., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab, Inc is required to disclose the following information to the government for the account listed in Attachment A from November 1, 2021 to January 3, 2024:

1. All subscriber/account information, including:
    a. Subscriber data, unrestricted by date, associated to the Kik account
    b. Current first and last name
    c. Email address
    d. Phone number
    e. Link to the most current profile picture
    f. Device related information
    g. Account creation date and Kik version
    h. Birthdate and email address used to register the account
    i. User location information
2. IP addresses associated to the Kik account, including remote port information
3. All chat logs associated to the Kik account
4. All messages sent from the Kik account to any other Kik users

5. All images and videos associated to the Kik account (to include images taken using the Kik app's camera, shared with the user's friends, or in a group chat or individual chat), including the unknown usernames and IP address associated to the sender of the images and videos and metadata associated with such images or videos
6. All other records of communications and messages made or received by the user
7. All activity logs for the account and all other documents showing the user's posts, chats, and other activities on Kik
8. A complete list of the identified Kik account's contact list and chat partners, deleted and undeleted
9. A date-stamped log showing the usernames that the Kik account added and/or blocked
10. All Kik chat groups in which the identified account is a member
11. All user-typed messages, audio notes, and video notes to friends within the Kik app using the chat feature
12. All user saved messages
13. All records of Kik searches performed by the account
14. All device-level location services maintained by Kik
15. The types of service utilized by the user
16. All abuse reports associated to the Kik account, including the unknown usernames
17. All emails associated to the Kik account

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

## II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2251(a) – production of child pornography and 18 U.S.C. § 2252A(a)(5)(B) - possession of child pornography, involving the user of Kik account **cabsnztrouble_6c5** from November 1, 2021 to January 3, 2024, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Any information and or images/videos which visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. The identity of the person who created or used the user ID, including records that help reveal the whereabouts of such person.

3. The identity of the person(s) who communicated with the user ID about matters relating to the enticement or kidnapping of children, the sexual exploitation of children, the distribution or receipt of child pornography, or the possession of child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the

disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.